

Review Location:

Reviewer:

Date of Review:

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
1.0 Documentation (InfoSec Docs)									
1.1	Security Policy						X	X	R
1.2	Incidence Response Plan						X	X	R
1.3	Disaster Recovery Plan (DRP) including natural disasters (flood, hurricane, earthquake, fire, etc)						X	X	R
1.4	Access Control Documentation						X	X	R
1.5	Backup Plan						X	X	R
1.6	Key control is logged, maintained, and reviewed						X	X	R
2.0 Safety									
2.1	Emergency exits are present and clearly marked						X	X	A
2.2	Emergency lights with backup power						X	X	A

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
2.3	Safety inspection sticker is current						X	X	A
3.0 Physical Access									
3.1	Picture identification is present and visible						X	X	R
3.2	Badge is present and visible						X	X	A
3.3	Visitors Sign In/Out Log						X	X	R
3.4	Badge control policies in place						X	X	A
3.5	Smart Card logs Badge logs are maintained and audited						X	X	A
3.6	Access card or token swiped or presented at automated reader for building/secure area entry or presentation of access card to security personnel required for building/secure area entry						X	X	R
3.7	Key control is logged, maintained, and reviewed						X	X	A

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
3.8	Authorized personnel access list is displayed inside the Data Center (DC) door						X	X	A
3.9	Data backup tapes are securely stored on-site until moved to off-site facility						X	X	A
3.10	Data backup tapes are securely stored off-site						X	X	A
3.11	Deposits and withdrawals of tapes and other storage media from the data backup library is authorized and logged						X	X	A
3.12	Unattended terminals are password protected						X	X	A
3.13	Password protected screen saver is set to turn on automatically after 15 minutes of inactivity						X	X	A
4.0 Facilities									
4.1	Windows protected by Intrusion Detection Systems (IDS) if less than 18 feet from ground or roof level						X	X	R

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
4.2	Openings over 96 square inches covered by material the same as the wall or by iron bars, or 18 gauge wire mesh						X	X	R
4.3	Individual personnel must have access to restricted areas (must not allow piggybacking or entry to unauthorized individuals)						X	X	R
4.4	Entrance doors must be constructed of solid wood, metal, or metal clad						X	X	R
4.5	Emergency doors will be void of all devices on the outside thereby allowing exit but no entry						X	X	A
4.6	Emergency doors will be equipped with emergency bar openers on the inside with a deadbolt throw of at least ½ inch						X	X	R

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
4.7	Doors have hinges on the inside. If door hinges are on the outside, the hinges must be peened, welded or equipped with setscrew fastener						X	X	R
4.8	Simple magnetic alarm switch should be placed on the protected side of doors, windows, or other moveable openings greater than 96 square inches to protect against movement						X	X	A
4.9	Walls, solid and contained from true floor to next floor or roof						X	X	A
4.10	True Floor to ceiling walls constructed of a material that would provide detections of surreptitious entry						X	X	A
4.11	Building and secure areas are protected with true ceilings and true floors						X	X	A
4.12	Roving guard						X	X	A

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
4.13	Security lighting for all exterior doors						X	X	R
5.0 Environmental									
5.1	Appropriate fire extinguishers (levels A, B, C) are present with current inspection information						X	X	A
5.2	Heat Ventilation Air Conditioning (HVAC) is present and working						X	X	A
5.3	Water sprinklers are present and in working condition						X	X	A
5.4	Heat and smoke sensors are present and in working condition						X	X	A
5.5	Uninterrupted Power Supply (UPS) is present and in working condition						X	X	A
5.6	24 hour temperature monitor/alarm is present and working						X	X	A
6.0 Human Threat									
6.1	Internal threat policies/procedures in place						X	X	R

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
6.2	External threat policies/procedures in place						X	X	R
6.3	Sabotage policies/procedures in place						X	X	R
6.4	Power Outage policies/procedures in place						X	X	R
7.0 Mobil Computing Devices									
7.1	Unattended portable and wireless devices are secured and locked						X	X	A
7.2	Unattended removable media containing sensitive information is secured and locked						X	X	A
8.0 Sensitive Data									
8.1	Sensitive data should be erased from whiteboards, removed from unsecured areas, and be properly disposed of						X	X	R

Nr.	Item	Y	N	N/A	Finding*	Recommendations	Disa/Nist Minimum Security Standard for Restricted Areas	Best Practice	Required/ Addressable (R/A)
9.0 Hard Copy Output Access									
9.1	Hard copy sensitive information that is no longer required is shredded or destroyed						X	X	R
9.2	All sensitive hard copy output is immediately picked up from output devices						X	X	R
9.3	All sensitive hard copy output is secured and locked						X	X	R
10.0 Marking									
10.1	Sensitive data is marked with the appropriate security label						X	X	R
11.0 Incident Response									
11.1	Incident Response Plan/Procedure						X	X	A
11.2	Computer Emergency Response Team (CERT)						X	X	A